ISSN 1727-1584. ПРАВО І БЕЗПЕКА. 2017. № 1 (64)

УДК 343.1+004

А. А. РУСЕЦЬКИЙ,
кандидат юридичних наук, доцент,
депутат Харківської обласної ради VII скликання;

Д. А. КУЦОЛАБСЬКИЙ,
курсант факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ ПОНЯТЬ «КІБЕРЗЛОЧИН» І «КІБЕРЗЛОЧИННІСТЬ»

Проаналізовано поняття «кіберзлочин» і «кіберзлочинність», які використовуються в науковій юридичній літературі, та охарактеризовано основні види кіберзлочинів.

Ключові слова: *кіберзлочин, кіберзлочинність, віртуальний простір, кібертероризм, комп'ютерні мережі.*

Rusetskyi, A.A. and Kutsolabskyi, D.A. (2017), "Theoretical and legal analysis of the concepts of «cybercrimes» and «cybercrime»" ["Teoretyko-pravovyi analiz poniat «kiberzlochyn» i «kiberzlochynnist»"], *Pravo i Bezpeka*, No. 1, pp. 74–78.

Постановка проблеми. На сьогодні в Україні та світі спостерігається стрімкий розвиток інформаційно-телекомунікаційних технологій, який призводить до змін в економічній, соціальній, культурній і політичній сферах. З одного боку, такий динамічний розвиток є дуже позитивним, однак з іншого, використання комп'ютерних технологій із корисливих та інших мотивів може становити не лише особисту небезпеку для громадян, їх службової діяльності, суспільного порядку, моральності, а й створювати загрозу національній безпеці держави та світу в цілому.

Про небезпечність, значущість та актуальність дослідження феномена кіберзлочинності також свідчать положення законів України «Про боротьбу з тероризмом» і «Про основи національної безпеки України». Так, згідно зі ст. 1 закону України «Про боротьбу з тероризмом» технологічний тероризм як злочин, що вчиняється з терористичною метою із застосуванням комп'ютерних систем і комунікаційних мереж, створює умови для аварій і катастроф техногенного характеру [1]. Відповідно до ст. 7 закону України «Про основи національної безпеки України» на сучасному етапі одними з основних реальних і потенційних загроз національній безпеці України, стабільності в суспільстві та в інформаційній сфері є комп'ютерна злочинність і комп'ютерний тероризм [2].

Слід також звернути увагу, що на сьогодні цей вид злочинності набуває глобального масштабу, оскільки необмежений доступ до мережі Інтернет, використання інформаційних технологій у повсякденному житті, легкість швидкого збагачення зваблюють все більше людей долучатися до такої злочинної діяльності.

Стан дослідження. Окремі питання кіберзлочинності неодноразово були предметом наукових досліджень як вітчизняних, так і зарубіжних учених. Зокрема, цій проблематиці присвячені праці О. Амеліна, Ю. Батуріна, В. Бутузова, В. Голубєва, О. Дзьобаня, В. Дзюндзюка, Р. Калюжного, М. Карчевського, М. Кравцової, В. Лісового, В. Навроцького, В. Номоконова, Д. Пашнєва, В. Пилипчука, М. Погорецького, В. Сташиса, В. Шеломенцева, О. Юрасова та інших.

Отже, **метою** нашої статті є проведення аналізу наукових праць і норм чинного законодавства щодо визначення понять «кіберзлочин» та «кіберзлочинність» і характеристика основних видів кіберзлочинів.

Виклад основного матеріалу. У чинному законодавстві України на сьогодні відсутнє нормативно-правове закріплення ключових термінів «кіберзлочин» і «кіберзлочинність», що спричиняє численні наукові дискусії серед дослідників сучасності. Науковці приділяють багато уваги дослідженню зазначеної проблематики та пропонують власні визначення цих понять. Так, кіберзлочином слід вважати втручання в роботу телекомунікаційних мереж, комп'ютерних програм, що функціонують в їх середовищі, або несанкціоновану модифікацію комп'ютерних даних, зухвалу дезорганізацію роботи критично важливих елементів інфраструктури держави, що створює небезпеку загибелі людей, завдання значної майнової шкоди або настання інших суспільно небезпечних наслідків, здійснювані з метою порушення суспільної безпеки, залякування населення або впливу на ухвалення органами влади вигідних злочинцям рішень, задоволення їхніх майнових або інших інтересів [3, с. 12].

Крім того, кіберзлочини визначають як сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення та використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [4, с. 7].

Варто звернути увагу, що в науковій юридичній літературі наведені такі ознаки кіберзлочинів, що відрізняють їх від «звичайних» злочинних посягань і значно підвищують їх суспільну небезпечність. По-перше, кіберзлочин не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого. По-друге, кіберзлочин є «автоматизованим» злочином (суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч). По-третє, суб'єкт кіберзлочину не підвладний обмеженням, які існують у реальному, фізичному світі. Так, кіберзлочини можуть бути вчинені моментально, а тому потребують швидкої реакції на них. По-четверте, кіберзлочинність і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це можливо стосовно злочинів, що вчиняються у реальному, фізичному світі [5, с. 130].

Виходячи з наведеного, можна зробити висновок, що кіберзлочин – це протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створювати особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці.

Таким чином, кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [6, с. 332]. Крім того, кіберзлочинність визначають як соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [7, с. 12].

Сучасні дослідники нерідко вважають поняття «кіберзлочинність», «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність» синонімами, однак існують і інші точки зору, за якими поняття «кіберзлочинність» є найширшим та охоплює найбільшу кількість злочинних посягань у віртуальному середовищі. Також використання поняття саме «кіберзлочинність» передбачає міжнародне законодавство [8, с. 173].

На наш погляд, справедливим є твердження, що кіберзлочинність є набагато ширшою за комп'ютерну злочинність, оскільки відображає не лише ті злочини, об'єктом і засобом посягання яких є комп'ютери, а й злочини, об'єктом посягання яких є інформація взагалі.

Основними ознаками кіберзлочинності є те, що:

1) кіберзлочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху локальними і глобальними комп'ютерними мережами, зберігаються в пам'яті будь-якого фізичного або віртуального пристроїв, спеціально призначених для їх зберігання, переробки та передачі. Крім того, кіберзлочини можуть вчинятися за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може бути як засобом вчинення, так і предметом злочину [6, с. 332];

2) кіберзлочинність має інтелектуальний характер – здійснення кіберзлочину вимагає певного набору знань, крім того інтелектуальність серед кіберзлочинців пропагується субкультурою хакерів, що дає їм стимул до розумового саморозвитку;

3) кіберзлочини, на відміну від інтелектуальних злочинів, доступні людям невисоких соціальних і вікових можливостей;

4) кіберзлочини є анонімними та неперсоніфікованими;

5) злочинця та жертву можуть розділяти тисячі кілометрів (віддаленість кіберзлочинів);

6) збиток від кіберзлочину часто здається жертві незначним порівняно з процедурою розслідування, яка здатна забрати час, але не гарантує притягнення до відповідальності винного та компенсації збитку (висока латентність кіберзлочинності) [9, с. 8].

Щодо класифікації кіберзлочинів, то вона також не має чіткого нормативно-правового закріплення. Так, відповідно до розділу XVI Кримінального кодексу України [10], який має назву «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», основними такими злочинами є: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363^1).

Відповідно до Конвенції Ради Європи про кіберзлочинність кіберзлочини можна умовно поділити на чотири групи: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення комп'ютерних даних, втручання в дані, втручання в систему, зловживання пристроями); 2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, та шахрайство, пов'язане з комп'ютерами); 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією); 4) правопорушення, пов'язані з порушенням авторських і суміжних прав [11, ст. 2–10].

Деякі науковці пропонують поділити кіберзлочини на агресивні та неагресивні. Так, до першої групи належать кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кібер-сталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група охоплює кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм [6, с. 333].

Дуже цікавою, на нашу думку, є класифікація кіберзлочинів, запропонована В. Б. Дзюндзюком і Б. В. Дзюндзюком:

1) злочини проти конституційних прав і свобод людини та громадянина, такі як порушення недоторканості приватного житла, порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, порушення авторських і суміжних прав;

2) злочини проти життя та здоров'я. Загрозливих масштабів у мережі Інтернет набуває наявність сайтів, які пропагують наркоманію, публікують технологію виготовлення наркотичних препаратів у домашніх чи промислових масштабах або які розповсюджують наркотичні засоби, психотропні речовини та їх аналоги;

3) злочини проти честі та гідності особи. Анонімність і широка аудиторія користувачів Інтернету дають безмежні можливості для розповсюдження інформації будь-яких видів, у тому числі наклепницької, такої, що порочить честь і гідність особи;

4) злочини проти власності. Одним із найпоширеніших видів злочинів на сьогодні є інтернет-шахрайство, нові форми, види і способи якого з'являються кожного дня;

5) злочини у сфері комп'ютерної інформації, такі як неправомірний доступ до інформації, створення, використання та розповсюдження шкідливих програм;

6) злочини проти суспільної моральності;

7) злочини проти безпеки держави. Із зростанням використання мережі Інтернет у державних структурах стає можливим нелегально дістати доступ не лише до приватної та корпоративної інформації, а й до інформації, що є

державною таємницею, також стає можливим скоювати такі злочини, як шпигунство, державна зрада або розголошення державної таємниці [9, с. 9–10].

Найпоширенішими видами кіберзлочинів у сучасному світі є:

– кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу, «трояни», «боти»);

– фішинг – клієнтам платіжних систем надсилаються повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи із проханням вказати свої рахунки та паролі;

– вішинг – у повідомленнях міститься прохання зателефонувати на певний міський номер, а під час розмови запитуються конфіденційні дані власника картки;

– онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

– піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;

– кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного телебачення;

– соціальна інженерія – технологія управління людьми в інтернет-просторі;

– мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

– протиправний контент – контент, що пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства;

– рефайлінг – незаконна підміна телефонного трафіка [12].

Варто взяти до уваги, що головне місце серед кіберзлочинів посідає кібертероризм як самостійний вид злочинної діяльності, який відрізняється від кіберзлочинності передусім своєю політичною спрямованістю, властивою тероризму в цілому [3, с. 12]. Під кібертероризмом слід розуміти навмисну політично вмотивовану атаку на об'єкти інформаційного простору (інформацію, що обробляється, комп'ютерну систему, мережу, а також на людину), що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної або суспільної безпеки, залякування населення, провокації військового конфлікту, чи загрозу вчинення таких дій [3, с. 13].

Отже, така значна кількість видів кіберзлочинів свідчить про те, що масштаби кіберзлочинності збільшуються. Тим самим зростає необхідність взаємодії держави із суспільством і міжнародною спільнотою з метою подолання цього негативного явища.

Висновки. Кіберзлочинність є вкрай небезпечним соціальним явищем, яке становить загрозу світового масштабу. На сьогодні боротьба з кіберзлочинністю є одним із пріоритетних напрямків діяльності правоохоронних органів держави, але для комплексної протидії їй необхідно, перш за все, узгодити на національному рівні та законодавчо закріпити термінологію, яка безпосередньо стосується кіберзлочинності, зокрема визначення ключових понять «кіберзлочин» і «кіберзлочинність».

Таким чином, удосконалення чинного законодавства дозволить визначити межі кіберзлочинності в Україні та правильно кваліфікувати дії осіб, які причетні до скоєння кіберзлочинів.

Список бібліографічних посилань

1. Про боротьбу з тероризмом: закон України від 20.03.2003 № 638-IV // База даних (БД) «Законодавство України»/Верховна Рада (ВР) України. URL: http://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 01.02.2017).

2. Про основи національної безпеки України: закон України від 19.06.2003 № 964-IV // БД «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/964-15 (дата звернення: 01.02.2017).

3. Пилипчук В. Г., Дзьобань О. П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети.* 2011. № 4 (21). С. 12–17.

4. Амелін О. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України.* 2016. № 3. С. 1–10. URL: http://www.chasopysnapu.gp.gov.ua/ua/pdf/11-2016/amelin.pdf (дата звернення: 05.02.2017).

5. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України.* 2010. № 3 (19). С. 129–136.

6. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.

7. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. … канд. юрид. наук: 12.00.08. Харків, 2016. 16 с.

8. Іванченко О. М. Кримінологічна характеристика кіберзлочинності, запобіганні кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. № 3. С. 172–177.

9. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. 12 с. URL: http://nbuv.gov.ua/j-pdf/DeBu_2013_1_3.pdf (дата звернення: 23.02.2017).

10. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-III // БД «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 20.01.2017).

11. Конвенція про кіберзлочинність: від 23.11.2001 // БД «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 17.01.2017).

12. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // Ресурсний центр ГУРТ: сайт. URL: http://www.gurt.org.ua/articles/34602 (дата звернення: 23.01.2017).

Надійшла до редколегії 06.02.2017

РУСЕЦКИЙ А. А., КУЦОЛАБСКИЙ Д. А. ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ ПОНЯТИЙ «КИБЕРПРЕСТУПЛЕНИЕ» И «КИБЕРПРЕСТУПНОСТЬ»

Проанализированы понятия «киберпреступление» и «киберпреступность», которые используются в научной юридической литературе, и охарактеризованы основные виды киберпреступлений.

Ключевые слова: *киберпреступление, киберпреступность, виртуальное пространство, кибертерроризм, компьютерные сети.*

RUSETSKYI A. A., KUTSOLABSKYI D. A. THEORETICAL AND LEGAL ANALYSIS OF THE CONCEPTS OF "CYBERCRIMES" AND "CYBERCRIME"

There is a rapid development of information technologies, which leads to changes in the economic, social, cultural and political spheres in the world including Ukraine. On the one hand, such dynamic development is very positive, but, on the other hand, the use of computer technologies can lead to harm to people, violation of public order, creating a threat to the national security of the country and the world in the whole.

The authors of the article point out that due to the lack of definitions of such key concepts as "cybercrimes" and "cybercrime" in the current Ukrainian legislation, scholars pay much attention to the research of these terms. Thus, cybercrimes they determine as: 1) interference in the work of telecommunication networks, computer software that function in their environment; 2) unauthorized modification of computer data; 3) the totality of socially dangerous actions connected with the violation of the right of ownership on information and information technologies, the right to receive and disseminate in time the reliable and complete information, etc.

Thus, cybercrime is understood as the totality of crimes that are committed in virtual space with the assistance of computer systems or by using computer networks and other ways of access to virtual space, as well as against computer systems, computer networks and computer data.

The improvement of the current legislation through the harmonization and consolidation of the main key concepts such as "cybercrime", "cybercrimes", "cyberterrorism", will allow us to define the boundaries of cybercrime as one of the dangerous social phenomenon on a global scale and adequately assess the actions of persons, who are involved in the commission of cybercrimes.

Keywords: *cybercrimes, cybercrime, virtual space, cyberterrorism, computer networks.*